Na bajt składa się 8 bitów. Na byt potrzeba 142 bajty. Taką długość ma najmniejszy wirus komputerowy.

KOMPUTER ZACHOROWAŁ

Komputer zawiesza się ostatnio zupełnie bez przyczyny. Dziwne. W dodatku jak gdyby wolniej działa i pojawiają się jakieś błędy na dysku. Po uruchomieniu systemu z dyskietki okazuje się, że nie jest dostępny dysk twardy. Czyżby wirus? Bingo! Program antywirusowy znajduje i usuwa niebezpiecznego wirusa. Tym razem udało się go unieszkodliwić zanim wyrządził szkody. Ale skąd ten wirus?

Obiegowa opinia głosi, że wirusy komputerowe piszą wyrzuceni z pracy informatycy na złość swoim szefom. Faktem jest, że pierwsze, powstałe w połowie lat osiemdziesiątych wirusy pisali zawodowi informatycy rozwścieczeni powszechnym i bezprawnym kopiowaniem owoców ich pracy. Obecnie masowym producentem nowych programów tego typu są uczniowie szkół podstawowych i średnich, powodując z roku na rok geometryczny wzrost liczby wirusów, szacowanej obecnie na 8500. Na szczęście przeważająca większość tej „twórczości" to prymitywne przeróbki już istniejących mikrobów, przez co nie sprawiają problemów w detekcji i usuwaniu. Od czasu do czasu pojawia się zupełnie nowa jakość, nowatorska konstrukcja, która drwi sobie z istniejących systemów zabezpieczeń i twórcy programów antywirusowych mają kilka gorących tygodni. Tworzą nowe, skuteczniejsze narzędzia i zabezpieczenia, które niestety trafiają również autorów wirusów. I tak w kółko.

WYŚCIG ZBROJEŃ

Dziesięć lat temu sprawa była prosta: program antywirusowy zawierał w sobie próbki kodu wirusa i przeglądał dysk twardy lub dyskietkę w poszukiwaniu charakterystycznych sekwencji. Po znalezieniu wirusa zbiór był skracany o długość intruza i poprawiany w odpowiednich miejscach.

Już po roku autorzy wirusów stworzyli wersje szyfrowane, w których tylko drobny fragment jest stały, a reszta za każdym razem wygląda inaczej. Metoda z sekwencjami nadal działała, ale pojawiły się problemy z identyfikacją wirusa, zaś identyfikacja jest konieczna, gdyż nawet drobne różnice w sposobie działania ukryte w tej zaszyfrowanej części mogą wpływać na sposób leczenia pliku.

Rok 1990 przyniósł nową jakość: wirusy polimorficzne. Nie dość, że szyfrują większość swojego kodu, to jeszcze procedura odszyfrowująca w każdej kopii jest inna. Są wirusy, które mogą generować miliardy różnych mutacji, w których praktycznie nie ma stałych elementów. Dotychczasowy sposób szukania sekwencji kodu zaczyna kuleć a czasem zupełnie zawodzi, tym bardziej, że niektóre wirusy pozostają zaszyfrowane nawet w pamięci, odkodowując się tylko na czas wykonywania.

Jak gdyby tego było mało, z czasem powstały specjalne programy wspomagające pisanie wirusów, takie jak Virus Creation Laboratory (VCL), Trident Polymorphic Engine, Dark Avenger's Mutation Engine czy Simulated Metamorphic Encryption Generator (SMEG). Dzięki nim autor tradycyjnych wirusów, a nawet zupełny amator, jest w stanie wyprodukować własnego, polimorficznego mikroba. Spowodowało to skrócenie czasu pracy nad przygotowaniem pojedynczego wirusa, a także znaczny przyrost liczby autorów. Wirusy stały się problemem nie tylko jakościowym, ale i ilościowym.

Odpowiedzią na to są programy antywirusowe stosujące tzw. analizę heurystyczną. Rozpoznają one wirusa nie po wyglądzie, lecz po zachowaniu. Dobry program tego typu potrafi nie tylko zidentyfikować konkretnego wirusa śledząc wykonywane przez niego czynności, ale też może wykryć, że obserwowany w pamięci podejrzany kod jest wirusem, mimo że nigdy wcześniej nie spotkał się z nim.

Kiedy już wydawało się, że sytuacja jest w miarę stabilna i trudno wymyślić coś nowego, okazało się, że Microsoft przygotował wszystkim Puszkę Pandory w postaci makr i programów w Visual Basicu, które mogą być dołączane do dokumentów i samoczynnie uruchamiać się po ich otwarciu. Uroczystego otwarcia dokonał w sierpniu zeszłego roku wirus WordMacro.Concept, i choć nie miał w sobie kodu destrukcyjnego, posłużył innym do produkcji własnych, już złośliwych wersji.

Wirusy dokumentów jako pierwsze w historii potrafią rozmnażać się niezależnie od typu proce-

FAKTY I MITY

Krąży wiele mitów dotyczących komputerowych wirusów. Im mniejszą mają ludzie możliwość sprawdzenia i zrozumienia istoty rzeczy, tym częściej uruchamiają swoją wyobraźnię. Część poniższego tekstu pochodzi z opracowania „Mity o wirusach komputerowych" (10 Październik 1993, autorzy: Rob Rosenberger, 74017.1344@compuserve.com i Ross M. Greenberg, greenber@ramnet.com) nadesłanego nam przez naszego Czytelnika, Dariusza Pindraszaka. Okazało się, że kilka akapitów trzeba było wyrzucić a kilka poprawić, gdyż w ciągu trzech ostatnich lat część mitów stała się faktem.

„Wszystkie destrukcyjne programy rozprzestrzeniają się jak wirusy".

– Nieprawda. Pamiętaj, „Koń Trojański" to ogólne określenie kodu mającego realizować cele destrukcyjne. Bardzo niewiele koni trojańskich kwalifikuje się do zaliczenia do grona wirusów. Reporterzy gazet i czasopism mają tendencję do nazywania wszystkiego wirusami, ponieważ zazwyczaj zupełnie nie rozumieją, czym jest przestępstwo komputerowe.

„Wirusy i konie trojańskie pojawiły się dopiero niedawno."

– Konie trojańskie można spotkać od pierwszych dni istnienia komputerów. Hakerzy bawili się wirusami już w początku lat sześćdziesiątych, traktując to jako formę zabawy. Wiele różnych technik opartych na koniach trojańskich stosowano do kradzieży pieniędzy, niszczenia danych, oszukiwania inwestorów itd. Informacje na ten temat nie docierały do opinii publicznej. Dopiero rewolucja komputerów IBM PC rzuciła światło na ten problem. Banki do dzisiaj ukrywają komputerowe włamania w obawie przed utratą zaufania swoich klientów.

„Tylko 500 różnych wirusów (dana z 1993 roku, obecnie szacuje się tę liczbę na 8500)? Przecież eksperci mówią o tysiącach."

– Eksperci podający znacznie większe liczby zazwyczaj pracują dla firm antywirusowych. Z powodów marketingowych odróżniają oni nawet najmniej istotne warianty. Gdy po raz pierwszy pojawił się wirus Marijuana, zawierał w sobie słowo „legalise". Niedługo potem pojawił się wariant, w którym słowo to zapisano jako „legalize". Każdy program, który wykrywał oryginalny wariant, mógł wykrywać wariant ze zmienioną jedną literą. Jednak firmy antywirusowe liczyły je jako „dwa" wirusy. Takie paranoiczne zliczanie szybko doprowadziło do astronomicznych liczb. Zauważ, że znakomita większość „nowych" wirusów to jedynie niewielkie modyfikacje doskonale znanych okazów.

„Wirus może zniszczyć wszystkie dane na moim dysku."

– Tak, i wylana filiżanka kawy może zrobić to samo. Możesz uratować swoje dane od problemu wirusa lub kawy, jeśli masz regularnie robione kopie zapasowe swoich danych. Kopia zapasowa oznacza różnicę pomiędzy drobną niewygodą a katastrofą. Możesz śmiało zakładać, że jest znacznie więcej przypadkowych strat danych niż powodowanych przez wirusy i konie trojańskie.

„Programy antywirusowe zabezpieczą mnie przed wirusami."

Nie ma czegoś takiego, jak absolutnie skuteczny program antywirusowy. Wirusy i inne konie trojańskie mogą (i są) być projektowane tak, by omijać pułapki zastawiane przez programy antywirusowe. Programy antywirusowe też nie są zawsze doskonałe i mogą zawierać błędy. Zawsze traktuj aktualne kopie zapasowe swoich danych jako główną broń przeciwko wirusom. Programy antywirusowe traktuj jako drugą linię obrony.

„Wirus może się schować w pliku danych."

Pliki danych nie mogą spustoszyć Twojego komputera – jedynie wykonywalne programy mogą to zrobić. Ale bądźmy realistami: to co uważasz za dane, może w istocie być wykonywalnym kodem. Przykładem mogą być pliki *.OVL, *.DRV, *.DLL, które są programami w pewnych sytuacjach wykonywanymi przez system. Podobnie rzecz się ma z dokumentami WMS Word-a 6.0, które również mogą zawierać w swoim wnętrzu wykonywalny kod.

„Mój komputer może się zarazić, jeśli zadzwonię do zarażonego BBS-u lub połączę się z Internetem."

BBS sam z siebie nie może zapisać żadnej informacji na Twoim dysku. Robi to wykorzystywane przez Ciebie oprogramowanie komunikacyjne. Jedynie Ty możesz ściągnąć zarażone programy do swojego komputera. Tak samo jest z Internetem.

„Mój komputer może się zarazić, jeśli kopiuje dane z zarażonej dyskietki."

To nieprawda. Zarazić się można tylko przy próbie startu systemu z zarażonej dyskietki, uruchamiając skopiowany z niej program lub wczytując zarażony dokument do Word-a lub Excel-a. Samo kopiowanie nie może spowodować zarażenia, gdyż nie uruchamia programów. Pamiętać należy, że KAŻDA dyskietka, nie tylko systemowa, nawet pozornie pusta, może zawierać niebezpiecznego wirusa.

sora i systemu operacyjnego. Złamały również żelazną zasadę, w myśl której tylko program mógł być źródłem infekcji. Połowa z około dziesięciu znanych obecnie wirusów dokumentów nie działa na innych niż anglojęzyczne wersje Word-a i Excel-a 6.0, ale mimo to mnożą się w szybkim tempie. Przyczyna tego faktu tkwi nie tyle w programach antywirusowych, które ostatnio coraz lepiej radzą sobie z tym typem wirusów, ale w świadomości ludzi, którzy jeszcze nie mają w zwyczaju sprawdzać przychodzących dokumentów przed otwarciem.

BAAARDZO ŚMIESZNE

Twórcom wirusów dopisuje poczucie humoru i miło jest stwierdzić, że nie są to sami nienawistni obłąkańcy. Pomysły bywają rzeczywiście zabawne: ktoś pisze zdanie i w momencie gdy stawia kropkę, zza ekranu wyskakuje robak, zjada ją i ucieka. I tak na okrągło. Po prostu nie sposób postawić kropki.

Innym kapitalnym efektem są obsypujące się literki. Podczas pracy z edytorem nagle zauważamy, że jedna z literek spadła z cichym stukiem. Kiedy ze zdziwieniem przyglądamy się jej, spada druga, trzecia... i w końcu wszystkie tworzą sporą kupkę na dole ekranu.

Jest wirus, który odwraca do góry nogami zawartość ekranu. Można nawet dalej pracować z komputerem, tylko trzeba przełożyć monitor „na plecy".

Oddzielną grupę tworzą wirusy wysyłające komunikaty do użytkownika: „Wykryto wodę w koprocesorze", „Nudzi mi się – DRUKARKA", „Wykryto dwie dyskietki w napędzie A:". Z wirusów wydających dźwięki (są takie, a jakże, niektóre nawet mówią) szalenie spodobał mi się pomysł nadawania o pełnych godzinach sygnału czasu.

Są też wirusy patriotyczne. Jeden taki rodzimy produkt wyświetla napis TERAZ POLSKA i pokazuje ładnie animowaną polską flagę... ale przedtem zeruje zawartość pamięci CMOS. Nietrudno przewidzieć, kogo będzie przeklinał Anglik czy Filipińczyk po spotkaniu tego wirusa.

Wbudowana w program MkS_Vir encyklopedia wirusów dostarcza setki takich przykładów, śmiesznych i mniej śmiesznych, albowiem bywa, że wirus zachowuje się obraźliwie. Jest w każdym razie co czytać i oglądać przez kilka godzin. Odnosi się po tym wrażenie, że ludzka pomysłowość nie ma granic i szkoda, że jest w tak bezmyślny sposób stosowana.

Być może czytają mnie osoby, które zamierzają napisać lub piszą wirusy. Nie zamierzam roztrząsać przyczyn dlaczego to robią – dla dowcipu, chęci imponowania, aby sobie coś udowodnić, czy też z czystej nienawiści do świata. Chciałbym, aby wiedzieli, że NIE MA NIESZKODLIWYCH WIRUSÓW. Większość szkód powodowanych przez wirusy komputerowe to przypadkowe uszkodzenia danych, wynikające z błędu w programie lub przyjęcia przez autora błędnych założeń. Na przykład wirusy dyskowe instalując się w tablicy partycji przenoszą jej oryginalną zawartość w inne, sobie tylko znane miejsce na dysku. Zdarza się nagminnie, że są to pewne nieużywane obszary początkowych sektorów dysku... ale tylko pod DOS-em. Ale w innych systemach operacyjnych, takich jak Windows NT, OS/2 czy UNIX (w których również można uruchamiać programy DOS-owe, czyli również wirusy) bywają tam przechowywane istotne informacje, które zostają bezpowrotnie stracone. Bywa też, że pewne triki doskonale działające u autora wirusa, w konstrukcjach nietypowych (ba, wystarczy na przykład dysk twardy nowszej generacji) nie działają, a nawet niszczą zawartość przypadkowych sektorów. A zatem pozornie niegroźny wirus, który ma być żartem, może siać zniszczenie i często do tego dochodzi. Autor wirusa MUSI być świadom, że ponosi odpowiedzialność nie tylko za zamierzone ale i niezamierzone zniszczenia, podobnie jak rodzice odpowiadają za szkody wyrządzone przez dzieci.

CYFROPATA

Wirus komputerowy jest cyfrowym psychopatą. Jeśli ma niszczyć, to niszczy – nigdy się nie lituje. Wirusy uderzają w najbardziej bezbronnych, bo doświadczeni komputerowcy umieją ich unikać. Zdarzają się wypadki tak krzywdzące, że programista z pewnością nie napisałby wcale wirusa – GDYBY JE PRZEWIDZIAŁ. Bywają sytuacje, w których autor wirusa z pewnością darowałby ofierze i zaniechał zniszczeń – ALE NIE MA JUŻ NA TO WPŁYWU.

Być może nie wzbudzają emocji szkody finansowe powodowane przez destrukcyjną działalność wirusów. Nie każdy pewnie przejmuje się też losem twórców, którzy nagle tracą miesiące czy lata pracy. Ale notowane są już przypadki, że niszczone są bazy danych chorych w szpitalu. Zdarzyło się również, że w wyniku uszkodzenia spowodowanego przez wirusa podano chorym złe leki, co kilku z nich mało nie kosztowało życia. Jak dotąd nie ma udokumentowanych przypadków śmierci, których bezpośrednią przyczyną byłaby działalność wirusa komputerowego (błędy w oprogramowaniu samolotów zebrały już krwawe żniwo), ale komputery wkraczają coraz bardziej w nasze życie i jest to tylko kwestia czasu.

Każdy autor wirusa jest potencjalnie tym pierwszym cyfrowym mordercą. I tak powinien być traktowany.

HARE

Gwiazdą tegorocznego sezonu ogórkowego był wirus Hare.8160. W mediach aż huczało o nowym, superniebezpiecznym programie, który 22 sierpnia skasuje zawartość dysków twardych. Okazało się jednak, że jakoś nikomu krzywda się nie stała i właściwie nikt prawie tego wirusa nie przyłapał. Być może właśnie krzyk, jaki podniósł się wokół niego spowodował, że udało się zapobiec rozprzestrzenieniu, albowiem możliwości tego wirusa stawiają go w rzędzie tych najbardziej niebezpiecznych.

Hare zaraża zarówno programy, jak i boot sektory i tablice partycji. Jest to zatem wirus dysko-wo-plikowy (tak jak Flip czy Ciyvil Defence Virus). Na dysku twardym zasadnicza część wirusa przebywa na nie używanych cylindrach technicznych, a w przypadku dyskietek wirus... doformatowuje sobie dodatkową ścieżkę. Ponadto zarówno część ładująca w boot sektorze lub tablicy partycji, jak i część główna są szyfrowane polimorficznie. Szyfrowanie to jest zrobione tak sprytnie, że przy zarażaniu nowego komputera wirus definiuje sobie lokalną postać i wszystkie kopie wirusa na tym jednym komputerze wyglądają tak samo. Przy pobieżnej, amatorskiej analizie można nie zauważyć, że jest to wirus polimorficzny i w efekcie usunąć wszystkie kopie... za wyjątkiem tej jednej, która była przyczyną infekcji i wygląda oczywiście zupełnie inaczej, bo przywędrowała z innego komputera.

Hare potrafi ukrywać swą obecność. Nie jest to nic nowego, lecz warto wiedzieć na czym polega: wirus śledzi odwołania komputera do dysku i w przypadku próby odczytania zawirusowanego pliku ulecza go na chwilę. Efekt jest taki, że nawet większość programów antywirusowych nie jest w stanie przyłapać wirusa na dysku. Zdarzały się nawet przypadki, że program antywirusowy,

RODZAJE WIRUSÓW

Podział ze względu na sposób przenoszenia:

Wirusy plikowe – najstarszy rodzaj wirusów. Doczepiają się do programów (czyli plików EXE, COM, SYS, BIN, OVL, MNU) w ten sposób, że przy próbie uruchomienia zarażonego programu najpierw uruchamia się kod wirusa, przejmuje częściowo kontrolę nad systemem i natychmiast uruchamia program nosiciela. Po tej niezauważalnej dla użytkownika infekcji wirus stara się powielać, czyli dopisać swoje kopie do innych programów zapisanych na dysku twardym lub dyskietce.

Wirusy dyskowo – zapisują się w boot sektorze lub tablicy partycji w miejscu istniejących tam specjalnych programów do uruchamiania systemu. Są wczytywane z dysku jako pierwsze i uruchamiane, a następnie same uruchamiają system operacyjny. Wirusem takim można zarazić się jedynie podczas próby startu systemu operacyjnego z zainfekowanej dyskietki (dyskietka z danymi lub zupełnie pusta może również zawierać wirusa). Jest to najbardziej rozpowszechniony obecnie typ wirusa.

Wirusy dyskowo-plikowo – potrafią zarażać zarówno programy jak i boot sektory. Łączą możliwości dwóch powyższych typów.

Wirusy dokumentów – pojawiły się w zeszłym roku, w postaci makr w programie MS Word 6.0. Potrafią samodzielnie dopisywać się do zapisanych na dysku dokumentów a nawet siać destrukcję. Mogą działać na różnych typach komputerów (PC, Mac) i niezależnie od systemu operacyjnego, gdyż ich środowiskiem jest Word 6.0 lub Excel 6.0 (lub nowsze).

RODZAJE WIRUSÓW

Podział ze względu sposób działania:

nierezydentne
po uruchomieniu programu-nosiciela wirus znajduje następną ofiarę, zaraża ją a następnie usuwa się z pamięci ustępując miejsca swojemu nosicielowi. W ten sposób działają najprostsze wirusy – mogą mieć tylko kilkadziesiąt bajtów.

rezydentne
po uruchomieniu przebywają w pamięci przez cały czas, starając się w sprzyjających momentach infekować co się tylko da.

ukrywające się
unowocześniona odmiana wirusów rezydentnych, które starają się ukryć swą obecność w pamięci a także zapobiegać odkryciu kopii na dysku.

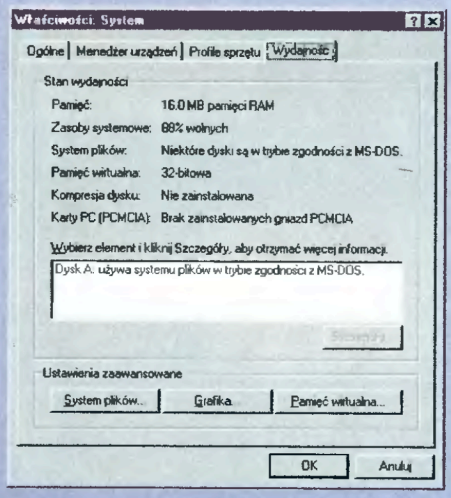
szyfrujące
zapisując się na dysku kodują zmiennym szyfrem zdecydowaną większość swego kodu, aby uniemożliwić wykrycie przez programy antywirusowe.

polimorficzne
potrafią mutować, czyli zmieniać swoją budowę w tak sprytny sposób, że kopia wirusa wygląda inaczej niż oryginał a mimo to działa tak samo. Najczęstszą metodą jest wstawianie w losowych miejscach nieistotnych, nic nie wnoszących kodów lub zastępowanie rozkazu lub sekwencji rozkazów innymi rozkazami o takim samym efekcie działania (np. odejmij A do A i zapisz 0 do A).

Niezależnie od sposobu przenoszenia czy działania wszystkie wirusy mogą w określonych sytuacjach podjąć zakodowanie w nich działania specjalne, najczęściej zamazujące zawartość dysku twardego lub wyświetlające efekty na ekranie.

przeglądając dokładnie cały dysk przyczynił się wydatnie do dokładnego jego zawirusowania. Dlatego właśnie ważne jest, aby przy szukaniu wirusów uruchamiać system operacyjny i program antywirusowy z czystej, zabezpieczonej dyskietki, aby mieć absolutną pewność, że w pamięci nie będzie żadnego sprytnego oszusta.

Hare jest chyba pierwszym wirusem, który radzi sobie z zabezpieczeniami Windows 95. Wszystkie wirusy pisane są w ten sposób, że infekują dyskietkę wtedy, gdy jest ona w użyciu. Gdyby próbowały zapisać się na dyskietce w przypadkowym momencie, taka nagła aktywność napędu na pewno wzbudziłaby nieufność użytkownika i cała konspiracja na nic. W tym celu wirusy w odpowiedni sposób śledzą aktywność komputera i wykrywają moment odwołania się do dyskietki. Ale Windows 95 posiada własne sterowniki obsługi dyskietek i tradycyjne procedury, te śledzone przez wirusy, wcale nie są używane. Efekt jest taki, że wirusy nie dowiadują się o tym, że w napędzie jest dyskietka i użytkownik z niej korzysta. Hare radzi sobie z tym w ten sposób, że kasuje z dysku plik systemowy IOSUBSYS\HSFLOP.PDR zawierający 32-bitowe sterowniki obsługi stacji dysków. Przy następnym uruchomieniu systemu, Windows 95 nie znajduje potrzebnego pliku i (nie informując użytkownika!) przestawia się automatycznie w DOS-owy tryb obsługi dyskietek. Informacje o tym fakcie można znaleźć jedynie w jednym z okien panelu sterowania.



Jakby tego było mało, wirus ten próbuje także metod zapisu na dysku twardym poprzez bezpośrednie odwołania do portów sterownika. W dodatku infekując tablicę partycji czy boot sektory przejmuje obsługę klawiatury i symuluje naciśnięcie Y – programy antywirusowe i BIOS-y, którym udało się zauważyć próbę zapisu i pytają użytkownika co zrobić, dają się często nabrać, że zgadza się on na to.

Wirus Hare pojawił się w trzech, różniących się drobnymi szczegółami konstrukcyjnymi wersjach: około maja Hare.7610 a w lipcu Hare.7750 i Hare.7786. Autor wirusa miał dla niego inną nazwę, HDEutanasia (coś jakby Uśmiercacz Dysków Twardych), o czym informuje dwa razy do roku, czyli 22 sierpnia i 22 września, wyświetlając komunikat >>**"HDEutanasia" by Demon Emperor: Hare Krsna, hare, hare...**<<. Po czym na potwierdzenie swych słów kasuje zawartość dysków twardych.

Osobom zdumionym przemyślnością i złośliwością tego programu śpieszę z wyjaśnieniem, że nie jest on ani najbardziej złośliwy, ani też specjalnie genialny. Stał się sławny, bo trafił na sezon ogórkowy w prasie. I nie ma sensu wpadać w panikę 22 września, bo w kolekcji tysięcy istniejących wirusów bardzo wiele atakuje określonego dnia i praktycznie żadnego dnia roku nie jesteśmy bezpieczni. Nie włączanie komputera określonego dnia czy też przestawianie daty nie jest metodą – trzeba nauczyć się zapobiegać infekcji, umieć walczyć z wirusami i być zabezpieczonym na wypadek ataku.

JAK ROZPOZNAĆ?

Gdy manifestują swoją obecność, jest już z reguły za późno. Dowiadujesz się, że właśnie skasowano dysk twardy, lub też, że został zaszyfrowany i trzeba poczekać 24 godziny na odszyfrowanie (po czym okazuje się, że z tym odszyfrowaniem to nieprawda).

Są pewne symptomy, które wskazują na obecność wirusa. Ich zestawienie znajduje się w ramce obok. Należy do nich podchodzić z rezerwą – przyczyną takich problemów może być wirus, ale nie musi.

Doświadczeni użytkownicy zauważają nietypowe działanie komputera, ale nawet oni (zwłaszcza oni) nie ufają swoim zmysłom – są wirusy, których obecności w żaden sposób nie da się zaobserwować... aż do dnia X. Dlatego ważne jest, aby profilaktycznie, raz na jakiś czas, sprawdzać komputer programem antywirusowym. Częstotliwość tych działań powinna być dobrana indywidualnie, zależnie od ważności istniejących na komputerze danych i stopnia narażenia danego komputera na infekcję.

Programy antywirusowe istnieją w wielkiej mnogości i stosują najróżniejsze techniki. Pan Marek Sell zdradził mi jedną z metod stosowanych w MkS_Vir: jest to „łapanie na wabia", polegające na stworzeniu wirtualnego dysku i symulacji zapisywania na nim programów. Wirus próbuje zainfekować taki dysk lub plik z programem i w ten sposób zdradza swoją obecność. Pozwala to łapać niektóre ukrywające się wirusy, które trudno jest wykryć innymi metodami.

Obok programów mających za zadanie wykryć i unicestwić wirusa, które można poprzez medyczne analogie porównać do szczepionek, są również programy pełniące funkcję przeciwciał. Sposobem działania przypominają one trochę swoich wrogów: również przebywają stale w pamięci i również monitorują odwołania do dysku. Ale tu kończy się podobieństwo. Skanują one wszystkie kopiowane pliki i uruchamiane programy, alarmując o napotkanych intruzach. Choć ich działanie lekko spowalnia komputer i czasem też powoduje fałszywe alarmy, jest to jedna ze skuteczniejszych form zabezpieczenia. Przeważająca większość infekcji jest powodowana przez „stare", dobrze poznane wirusy i taki program, nawet nie najnowszy, doskonale przed nimi chroni.

Nie ma idealnego zabezpieczenia. Dobrze jest stosować oba typy programów antywirusowych: rezydentnego strażnika jako pierwszą linię obrony przed pospolitymi intruzami i co pewien czas aktualny program skanujący, który może sobie pozwolić na czasochłonne analizowanie kodu. Jest dobrym zwyczajem używanie w tym celu programów dwóch różnych producentów, gdyż ostatnio bardzo często zdarza się, że autorzy wirusów umieszczają w swoich „dziełach" kod mający za zadanie wprowadzić w błąd lub ominąć zabezpieczenia konkretnych pakietów antywirusowych.

Tabela na dole strony to zestawienie najlepszych istniejących programów antywirusowych.

OBJAWY OBECNOŚCI WIRUSA

- Program uruchamia się wolniej niż zwykle.
- Nie ma dostępu do dysku twardego po uruchomieniu systemu z dyskietki.
- Program zmienił swoją długość na dysku.
- Polecenie CHKDSK pokazuje mniej niż 655360 wszystkich bajtów pamięci.
- Niespodziewanie brakuje miejsca na dysku twardym.
- Dysk twardy wykazuje aktywność bez powodu.
- Pod Windows pokazują się błędy operacji 32-bitowych.
- Litery na ekranie samodzielnie się przemieszczają.
- Komputer utracił zawartość pamięci CMOS, mimo że bateria działa poprawnie.
- Na dysku pojawiły się pliki niewiadomego pochodzenia lub o dziwnych nazwach.
- Podczas używania klawiatury z komputera dochodzą dźwięki.

Uwaga: *Niektóre z tych objawów są typowe dla pewnych programów lub komputerów. Niepokoić należy się wtedy, gdy pojawią się nagle, bez uzasadnionej przyczyny.*

☆☆☆☆☆ produkt bardzo dobry
☆☆☆☆ produkt dobry
Znak ✔ oznacza, że dany program posiada certyfikat NCSA (dane z dnia 9 września 1996), amerykańskiej agencji zajmującej się ochroną danych komputerowych.
Kolumny DOS, WIN i TSR informują, czy dany program posiada wersję dla DOS-u, MS Windows i rezydentny program strażniczy.
Z bardziej znanych programów brakuje w tym zestawieniu Microsoft Anti-Virusa. Z wykrywalnością rzędu 25% nie zasługuje nawet na jedną gwiazdkę.
ThunderByte ma miec niebawem polskiego dystrybutora a byc może nawet będzie spolszczony.

Nazwa:	AVAST!	AVP	AVScan	Dr Solomon's AVTK	F-Prot Professional	IBM AntiVirus	InocuLAN	Iris AntiVirus
Jakość	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆	✔☆☆☆☆	✔☆☆☆☆	✔☆☆☆☆	✔☆☆☆☆	☆☆☆☆
Producent:	Alwil Software	KAMI	H+BEDV	S&S	Command Software	IBM	Cheyenne Software	Iris Software
DOS	+	+	+	+	+	+	+	+
WIN	+	–	?	+	+	+	+	+
TSR	+	–	?	+	+	+	+	+
Internet:	http://www.anet.cz/alwil/	http://www.polbox.com.pl/vacimex/	e-mail:71310.3140@compuserve.com	http://www.drsolomon.com/	http://www.commandcom.com/	http://www.brs.ibm.com/ibmav.html	http://ftsa.cheyenne.com/	
Cena:		160 + VAT		495 zł + VAT	309 zł + VAT	49 USD		
Uwagi:	Znajduje, ale nie usuwa wirusów plikowych. Do usunięcia wirusa boot sektora wymaga wcześniejszej dyskietki ratunkowej	Uważany za najlepszy program skanujący. Wolny w działaniu. Przegląda archiwa. Doskonale radzi sobie z wirusami w pamięci.		Bardzo dobra wykrywalność wirusów w ostatnich testach.	Doskonała wykrywalność wirusów w ostatnich testach	Bardzo szybki (dzięki wykorzystaniu dodatkowych sum kontrolnych)	Przegląda niektóre archiwa	Nowość na rynku. Doskonale radzi sobie z wirusami w pamięci
Najbliższy dystrybutor:	ALWIL Trade s. s r.o. Czech Republic tel.: +42-2-7822547	VACIMEX Przedstawicielstwo PROVAC AG tel./faks: (022) 106246	H+BEDV Niemcy tel.: +49-7542-93040	Dagma sp. z o.o. tel./faks: (032) 1021122	POLAND Masters S.C. tel.: (033) 520755	IBM Polska tel.: (022) 6251010		

Ramka „Jak unikać wirusów?" zawiera kilka rad, dzięki którym uda się być może uniknąć konieczności sięgania po te programy.

WILD LIST

Od 1993 Joe Wells, pracujący jako konsultant IBM, prowadzi listę wirusów złapanych na wolności. Każdego miesiąca kontaktuje się z nim ponad czterdzieści osób z całego świata i informuje o wirusach spotykanych w ich regionie. Wśród tych osób znaleźć można całą śmietankę twórców programów antywirusowych, wśród nich także i Marka Sella.

Tabela obok pokazuje zestawienie 25 wirusów najbardziej rozpowszechnionych, stan z połowy tego roku. Jak widać 60% z nich należy do rodziny wirusów dyskowych, które mogą rozprzestrzeniać się jedynie przy próbie startu systemu z dyskietki, a więc unikanie tego typu działań znacznie zmniejsza ryzyko infekcji. Specjaliści twierdzą, że zmiana kolejności bootowania komputera na C: A: (czyli w efekcie wykluczenie możliwości startu systemu z dyskietki, jeśli dysk twardy działa) zmniejsza ryzyko infekcji o 80%.

Nazwa	Alias	Zasięg*	Typ
AntiEXE.A	D3, Newbug	100%	dyskowy
Form.A	Form 18	100%	dyskowy
One_Half.3544	Dis, Free Love	97%	dyskowo-plikowy
Concept	WM.Concept	94%	makro
Ripper	Jack Ripper	91%	dyskowy
Empire.Monkey.B	Monkey 2	88%	dyskowy
AntiCMOS.A	Lenart	84%	dyskowy
Junkie		81%	dyskowo-plikowy
Parity_Boot.B	Generic 1	81%	dyskowy
Natas.4744	Satan, Sat_Bug	78%	dyskowo-plikowy
Boot-437		75%	dyskowy
Michelangelo.A		75%	dyskowy
NYB	B1	75%	dyskowy
Sampo	Turbo, Wllop	72%	dyskowy
Stoned.Angelina.A		69%	dyskowy
Stoned.No_INT.A	Stoned	69%	dyskowy
Kampana.A	AntiTel,Campana	66%	dyskowo-plikowy
Die_Hard	DH2, Wix	63%	plikowy
V-Sign	Cansu, Sigalit	63%	dyskowy
Stoned.Standard.A	New Zealand	59%	dyskowy
Tequila.A		56%	dyskowo-plikowy
WelcomB	Bupt.9146	56%	dyskowy
Tai-Pan.438	Whisper	53%	plikowy
Cascade.1701.A	1701	50%	plikowy
Yankee Doodle.TP-44.A	RCE-2885	50%	plikowy

*) wartości orientacyjne

DEFINICJE

Wirus komputerowy – mały program potrafiący bez woli i wiedzy użytkownika komputera dopisać swoją kopię do innego programu komputerowego w taki sposób, że przy próbie jego uruchomienia uruchamiany jest także kod wirusa. Dzięki możliwości powielania się i korzystaniu z przenoszenia/przesyłania programów (dyskietki, sieć) może rozprzestrzeniać się i infekować rosnącą liczbę komputerów.

Inne rodzaje komputerowych intruzów:

Bakteria (po angielsku worm, czyli robak) – program korzystający z luk w ochronie systemów sieciowych i rozprzestrzeniający się w sieciach komputerowych bez udziału człowieka. Od wirusów różni się tym, że istnieje jedynie jako działający proces w pamięci operacyjnej, nie zapisuje swych kopii w pamięci masowej. Po wyłączeniu komputera „ginie". Najbardziej spektakularnym przykładem takiego programu jest twór Roberta Morrisa, który w roku 1988 niekontrolowanie rozmnożył się i zablokował na pewien czas większość amerykańskich ośrodków badawczych. Robert wyszedł już z więzienia, ale opłacenie 250 tys. USD odszkodowania to duże obciążenie, nawet dla zdolnego studenta informatyki.

Koń trojański – popularne na zachodzie, ale u nas rzadko spotykane ogólne określenie programu, który w tajemnicy lub wbrew woli użytkownika wykonuje pewne, zaprogramowane przez swego twórcę czynności. Zarówno wirus jak i bakteria są specyficznymi odmianami konia trojańskiego. W zeszłym roku mówiono, jakoby Windows 95 przy instalacji szpiegował zawartość twardych dysków, aby ewentualnie zawiadomić producenta o nielegalnych kopiach programów. Byłby to wspaniały przykład konia trojańskiego, gdyby nie fakt, że na szczęście (dla Microsoftu) jest to bzdura.

Dropper – specyficzna odmiana konia trojańskiego, w postaci programu, który ma za zadanie wprowadzić wirusa do systemu. Dropper różni się od zainfekowanego programu tym, że wirus został doń dołączony celowo przez autora i jest najczęściej dodatkowo zaszyfrowany. Droppery są podrzucane do BBS-ów lub popularnych list newsowych na Internecie, skąd ich użytkownicy ściągają je do domów zwabieni zachęcającymi nazwami: PKZIP300.EXE, VPRO46C.EXE czy COOLDEMO.COM.

JAK UNIKAĆ WIRUSÓW?

- Pliki z niepewnych źródeł należy przed pierwszym uruchomieniem sprawdzić programem antywirusowym. Trzeba pamiętać o tym, żeby mieć jak najnowsze wersje tych programów. Nowe, aktualne wersje programu antywirusowego pojawiają się z reguły raz w miesiącu, choć istnieją także aktualizowane co tydzień.
- Należy unikać uruchamiania systemu z dyskietki. Najlepiej jest zmienić w BIOS-ie kolejność bootowania systemu na C: A:, co wyklucza możliwość przypadkowego uruchomienia wirusa z boot sektora dyskietki. Niestety nie wszystkie BIOS-y umożliwiają taką zmianę.
- Należy mieć kopie zapasowe zawartości dysku twardego, przede wszystkim tych jego fragmentów, których nie da się odtworzyć: prac, dokumentów a zwłaszcza archiwów.
- Na wypadek infekcji należy zawczasu przygotować specjalną dyskietkę systemową, która zawiera program antywirusowy i kopię zapasową początkowych obszarów dysku. Kopia taka przydaje się w przypadku nieusuwalnych wirusów boot sektora lub tablicy partycji i można ją wykonać za pomocą większości programów antywirusowych (np. MkS_Vir-a).
- Pliki pobieraj tylko z renomowanych BBS-ów i takich miejsc w Internecie, w których istnieje pewność, że są nadzorowane i sprawdzane programami antywirusowymi. Nie należy także pobierać zbyt nowych plików – warto poczekać z tydzień, niech inni sprawdzą na sobie, czy wszystko jest w porządku.

Jedna z prastarych mądrości mówi, że mężczyzna musi zbudować dom, zasadzić drzewo i mieć syna. Podobnie każdy komputerowiec musi złożyć peceta, nauczyć się asemblera i stworzyć wirusa. Niestety z tym wirusem jest dokładnie tak samo jak z synem: frajda tworzenia jest tak duża, że zapomina się o odpowiedzialności.

Wojciech JABŁOŃSKI

McAfee Scan	MkS_Vir	Norman Virus Control	Norton AntiVirus	Sweep	ThunderBYTE	VET	Virus ALERT!	Vi-Spy
✔☆☆☆☆	☆☆☆☆	☆☆☆☆	✔☆☆☆☆	☆☆☆☆	✔☆☆☆☆	☆☆☆☆	☆☆☆☆	☆☆☆☆
McAfee Associates	Apexim	Norman	Symantec	Sophos	ESaSS	Cybec Pty Ltd	Look Software	RG Software
+	+	+	+	+	+	+	+	+
+	–	+	+	+	+	+	+	+
+	–	+	+	+	+	+	+	+
http://www.mcafee.com/	http://www.atm.com.pl/~apeximwa/	http://www.norman.com/	http://www.symantec.com/	http://www.sophos.com/	http://www.thunderbyte.com/	http://www.cybec.com.au/	http://www.look.com/	http://www.rg-av.com/
65 USD	59 + VAT		148 USD + VAT	195 GBP		59 GBP	70 USD	75 USD
Popularny w USA (ok. 25% rynku)	Produkt rodzimy. Szybko reaguje na pojawiające się w Polsce wirusy	Bardzo dobry w wykrywaniu wirusów polimorficznych.	Bardzo popularny w USA (ok. 60% rynku)	Znajduje, ale nie usuwa wirusów plikowych.	Wyróżnia się dużą szybkością przeszukiwania i doskonałą wykrywalnością. Zdarzają się fałszywe alarmy.	Szybko przeszukuje dysk twardy.	Znajduje, ale nie usuwa wirusów plikowych. Do usunięcia wirusa boot sektora dysku twardego wymaga wcześniejszej dyskietki ratunkowej.	
	APEXIM S.A. dział MkS_vir'a tel.: (022) 470832	Norman Niemcy tel.: +49-212-267190	TCH Components tel.: (022) 487172	Safe Computing Ltd tel.: (022) 619 8956	ESET s.r.o Słowacja tel.: +42-7-2048228	VET Anti-Virus Software Wielka Brytania tel. +44-114-2757501		Hi Tech Marketing Serv., Wielka Brytania tel.: +44-161-9415073